	Application No.	Applicant(s)
Notice of Allowability	09/617,913	REECE, RICHARD W.
	Examiner	Art Unit	
	Ponnoreay Pich	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *10/18/2004*.

2. ☒ The allowed claim(s) is/are *6-18*.

3. ☒ The drawings filed on *17 July 2000* are accepted by the Examiner.

4. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a) ☐ All   b) ☐ Some*   c) ☐ None   of the:

        1. ☐ Certified copies of the priority documents have been received.

        2. ☐ Certified copies of the priority documents have been received in Application No. _____ .

        3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

    * Certified copies not received: _____ .

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application. **THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.**

5. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

6. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.

    (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached

        1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____ .

    (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of

    Paper No./Mail Date _____ .

    Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

7. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☒ Notice of References Cited (PTO-892)

2. ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)

3. ☐ Information Disclosure Statements (PTO-1449 or PTO/SB/08), Paper No./Mail Date _____

4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material

5. ☐ Notice of Informal Patent Application (PTO-152)

6. ☒ Interview Summary (PTO-413), Paper No./Mail Date *2005* .

7. ☒ Examiner's Amendment/Comment

8. ☒ Examiner's Statement of Reasons for Allowance

9. ☐ Other _____ .

DETAILED ACTION

A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 10/18/2004 has been entered.

In the communication filed on 10/18/2004, applicant cancelled claims 1-5. Claims 6-7 were amended. Claims 8-18 were added. Claims 6-18 have been examined.

The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

Docketing

Please note that the application has been redocketed to a different examiner. Please refer all future communications regarding this application to the examiner of record using the information supplied in the final section of this office action.

Response to Arguments

Applicant's arguments filed on 10/18/2004 were directed towards base claims 6, 8, and 18. Applicant's arguments are based on new amendments added to the claim set filed on 10/18/2004. The examiner will in the course of evaluating the claims consider the amendments and any new issues they bring up.

Response to Amendment

Applicant's amendments have been considered. Note that the previous office

actions are incorporated by reference in this office action and will be referred to as

necessary.

EXAMINER'S AMENDMENT

An examiner's amendment to the record appears below. Should the changes

and/or additions be unacceptable to applicant, an amendment may be filed as provided

by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be

submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview

with Joseph Colaianni on 4/28/2005 and on 5/4/2005.

Please replace the paragraph starting on page 7, line 7 with the following:

The Maurer and Cachin proposal possibly resolves some for the drawbacks

noted for quantum cryptography and the embodiments of U.S. patent 5,161,244. More

particularly, the common broadcast allows universal access, suggesting that many

users could use the same broadcast and thus reduce the cost of implementation. In

addition, the larger the gap between the adversary's memory and the broadcast string

of random numbers the lower the amount of information that must be transferred

between individual users.

Please replace the paragraph starting on p23, line 22 with the following:

It is an advantage of the present invention that many devices of varying

processing capability may be used. Therefore, although a typical embodiment is

represented by a conventional personal computer with a satellite downlink receiver,

108n is better defined by its function than by its specific hardware. For the purposes of

brevity the computers for encryption or decryption may be conventional personal

computers and are identified as an encryption station and decryption station

respectively. In view of this, the general requirements of the User Computing System

108n are enumerated as (a) through (f) as follows:

Please replace claims 6-7, 9-10, and 18 as follows:

Claim 6:

A method for encrypting data comprising:

>   broadcasting a random number sequence greater than N bits;

>   broadcasting a synchronization signal;

>   generating a private key;

>   providing said private key to an encryption station and to a decryption station;

>   receiving said random number sequence at said encryption station and said

decryption station;

>   receiving said synchronization signal at said encryption station and at said

decryption station;

selecting at time t an encrypting subsequence from said random number

sequence received at said encryption station, said selection time t based on said

synchronization signal received at said encryption station and on said private key;

filling an encryption reservoir with data from said encrypting subsequence;

updating a bit count of said encryption reservoir in accordance with said filling;

generating another selection time t' based on at least said encrypting

subsequence;

selecting at time t' another subsequence from said random number sequence

received at said encryption station;

additionally filling said encryption reservoir with data from said another

subsequence;

updating said bit count of said encryption reservoir based on said additionally

filling;

updating said selection time t' to represent a future time, based on at least said

another subsequence;

repeating said selection at time t', said additional filling, said updating said

encryption reservoir bit count, and said updating said selection time t' until said

encryption reservoir bit count reaches a predetermined fill value based on a

predetermined value N;

establishing an N-bit encryption key based on said encryption reservoir;

providing a message symbol sequence to said encryption station;

encrypting said message symbol sequence, at said encryption station, based on said N-bit encryption key, into an encrypted symbol sequence.

Claim 7:

A method for encrypting data according to the claim 6, further comprising:

generating an N-bit decrypting key at said decrypting station, identical to said N-bit encrypting key, said generating including

(a) selecting at said time t said encrypting subsequence from said random number sequence received at said decryption station, said selection time t based on said synchronization signal received at said decryption station and on said private key,

(b) filling a decryption reservoir with data from said encrypting subsequence,

(c) updating a bit count of said decryption reservoir in accordance with said filling,

(d) generating another selection time t' based on at least said another subsequence,

(e) selecting at time t' another subsequence from said random umber sequence received at said decryption station,

(f) additionally filling said decryption reservoir with data from said another subsequence,

(g) updating said bit count of said decryption reservoir based on said additionally filling,

(h) updating said selection time t' to represent a future time, based on at least said another subsequence,

(i) repeating (e) through (h) until said decryption reservoir bit count reaches a predetermined fill value based on a predetermined value N, and

(j) establishing an N-bit decryption key based on said decryption reservoir;

transmitting said encrypted message symbol sequence from said encryption station to said decryption station; and

decrypting said encrypted message symbol sequence, at said decryption station, based on said decrypting key, into said message symbol sequence.

Claim 9:

A method for generating an N-bit encrypting key, comprising:

broadcasting a random number sequence having significantly greater than N bits;

generating a private key;

providing said private key to an encrypting station;

receiving said random number sequence at said encrypting station;

generating an encrypting station sampling start time t based on said private key;

sampling a plurality of bits from said random number sequence received at said encrypting station, over a time interval based on said encrypting station sampling start time t, said plurality being less than N bits;

filling an encryption key reservoir at said data encryption station based on said sampled plurality of bits;

generating an updated encrypting station start time t', based on at least said plurality of bits;

sampling another plurality of bits from said random number sequence received at said encrypting station, over a time interval based on said updated encrypting station sampling start time t', said plurality being less than N bits;

further filling said encryption key reservoir based on said another plurality of bits from said transmitted random sequence;

repeating said generating an updated encrypting station start time t', said sampling another plurality of bits, and said further filling said encryption key reservoir until said encryption key reservoir reaches a predetermined bit count based on N; and

setting said N-bit encrypting key based on said encryption key reservoir.

Claim 10:

A method according to claim 9, further comprising generating an N-bit decrypting key identical in value to said N-bit encrypting key, said generating comprising:

providing said private key to a decrypting station;

receiving said random number sequence at said decrypting station;

generating a decrypting station sampling start time td based on said private key, said generating performed such that said decrypting station sampling start time td is identical to said encrypting station sampling start time t.

sampling a plurality of bits from said random number sequence received at decrypting station, over a time interval based on said decrypting station sampling start time td, said plurality being less than N bits;

filling a decryption key reservoir at said data decryption station based on said sampled plurality of bits;

generating an updated decrypting station sampling start time td', based on at least said plurality of bits;

sampling another plurality of bits from said random number sequence received at said decrypting station, over a time interval based on said updated decrypting station sampling start time td', said plurality being less than N bits.

further filling said decryption key reservoir based on said another plurality of sampled bits;

repeating said generating an updated decrypting station sampling start time td', said sampling another plurality of bits, and said further filling said decryption key reservoir until said decryption key reservoir reaches a predetermined bit count based on N bits; and

setting said N-bit decrypting key based on a value of said decrypting key reservoir,

wherein said generating a decrypting station sampling start time td, said filling a decryption key reservoir, said generating an updated decrypting stating sampling start time td', said further filling said decryption key reservoir, and said repeating are performed such that said decryption key reservoir and said encryption key reservoir are identically filled.

Claim 18:

A method for encrypting data, comprising:

broadcasting a random number sequence greater than N bits;

providing a private key to a first communication station;

receiving said random number sequence at said first communication station;

repeatedly filling a first reservoir at said first communication station with selected bits from said received random number sequence, each selection based on at least one of said private key and a value of previously selected bits, until said first reservoir reaches a predetermined threshold based on N;

setting an N-bit encryption key based on the content of said first reservoir;

inputting an information data; and

encrypting said information data into an encrypted data based on said N-bit encryption key.

Allowable Subject Matter

Claims 6-19 are allowed.

The following is an examiner's statement of reasons for allowance:

Claim 6:

As per claim 6, the applicant amended the claim to include a limitation which recites, "selecting at time t a subsequence from said random number sequence received at said encrypting station, said selection time t based on said synchronization signal received at said encryption station and on said private key." The examiner recognizes that random number generators with a seed value are well known in the art. The examiner also recognizes that random number generators can be used to generate

random time values. However, the examiner could not find a teaching or motivation in the prior art which would suggest why one of ordinary skill in the art that the time the applicant's invention was made would use an encryption key as a basis for the selection time for sampling a subsequence of random numbers. The only motivation the examiner could come up with for why one of ordinary skill would use a key as the basis for the sampling time in the field of the applicant's invention was disclosed by the applicant already.

The examiner was also not able to find in the prior art filling a reservoir until the reservoir reaches a predetermined threshold **based on N**; N is also the number of bits in the encryption key. The examiner did find prior art which disclosed a reservoir to hold random number values which were used for keys. However, the prior art was silent on the threshold value of the reservoir being based on N. In the prior art, the reservoir was filled to with an arbitrary number of random values or the reservoir was filled until the reservoir was full based on the capacity of the memory used.

Claim 9:

Claim 9 contains limitations substantially similar to claim 6 which the examiner was not able to find in the prior art. Claim 9 recites, "generating an encryption station sampling start time t based on said private key." Claim 9 also contains the limitation wherein the fill value for a reservoir is based on N; N is also the number of bits in the encryption key. The examiner believes claim 9 is allowable for the same reasons given for claim 6.

Claim 18:

As per claim 18, the examiner was not able to find in the prior art filling a reservoir until the reservoir reaches a predetermined threshold based on N; N is also the number of bits in the encryption key

Claims 7-8 and 14-16:

Claims 7-8 and 14-16 depend from claim 6.

Claims 10-13 and 17:

Claims 10-13 and 17 depend from claim 9.

Claim 19:

Claim 19 depends from claim 18.

Conclusion

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Ponnoreay Pich whose telephone number is 571-272-7962. The examiner can normally be reached on 8:00am-4:30pm Mon-Fri.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 571-272-3859. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the

Patent Application Information Retrieval (PAIR) system. Status information for

published applications may be obtained from either Private PAIR or Public PAIR.

Status information for unpublished applications is available through Private PAIR only.

For more information about the PAIR system, see http://pair-direct.uspto.gov. Should

you have questions on access to the Private PAIR system, contact the Electronic

Business Center (EBC) at 866-217-9197 (toll-free).

PP

KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100